(delegated certificates). By way of illustration and not by way of limitation, specific ticket contents and methods for verifying and authenticating tickets and keys are given in the description.

Similarly, the listed components of a device show the preferred embodiment of the present invention, and other configurations are also possible. For example, instead of placing the confirmation input device on the key device, it can be placed on the control device, which then forwards the confirmation to the key device. For another example, a key device might have an LCD display that shows the tickets that have been stored to the device.

Similarly, lists of information that a device may contain describe the preferred embodiment of the invention. The embodiment of the present invention can be adapted for a variety of needs by varying the information present on devices (including, but not limited to, the variation possibilities given by the lists of optional information). For example, storing user names on key devices is useful, but not essential. Adding information to devices allows a number of specialized uses. For example, by adding a social security number and the public key of the key device, both digitally signed by a state agency, a key device can be used for identification purposes.

The embodiment of invention preferably uses Bluetooth security features (specifically the different types of link keys and their use) and public key cryptography. Information about Bluetooth is available from **http://www.bluetooth.com/,** and a good starting point for public key cryptography is the Usenet cryptography FAQ at e.g. **http://www.landfield.com/faqs/cryptography-faq/.** Other communication systems can also be used.

It should be noted that whenever digital signatures by a "well-known trusted authority" are spoken of, the signatures can be chained so that there is one known central authority, who gives out authorizations to other organizations to create signatures. The authorization is then in the form of the public key of the receiving organization, encrypted with the private key of the central authority. The organization can then sign information with its own secret key, and enclose the authorization from the central authority.

The authenticity of the information can be checked by first decrypting the authorization with the (well-known) public key of the central authority (proving the organization has the right to produce signatures), using the resulting public key of the organization to decrypt the signature (proving that the signature is produced by the organization the authorization is for), and checking that the signature matches the information (proving that the information has not been tampered with). In this way, one only has to know the public key of the central authority to check the authenticity of any information, but the central authority does not itself have to sign all the information - it can delegate that to other trusted parties which do not have to be well-known.

A key device (hereafter KD) consists of a power source, a processing unit, storage (volatile and non-volatile memory), a communication device (preferably a Bluetooth wireless communication device), a confirmation input device (e.g. a button) and a confirmation request output device (e.g. a LED light). It may also have an emergency power socket that can be connected to a similarly equipped lock device (hereafter LD). A KD may further have a motion detector that allows it to switch off in order to conserve power when the KD is not moving. A KD may also have additional output devices for signaling success, failure, low power etc.

A KD stores the following information:

- A unique key device identifier, hereafter KID. A KID may or may not be changeable. Using e.g. the Bluetooth device address would make duplicating KDs impossible.
- A Unit Key (as per Bluetooth specification).
- A code used for controlling the KD, hereafter KD PIN code.
- An RSA key pair.
- The tickets of the user (maximum number may vary)-
- User name.
- Optionally, a KD may also store the following information:
- List of lock device identifiers for the LDs the KD can open, possibly also their human-readable names.
- Combination keys (as per Bluetooth specification) of LDs.
- User information, such as employee number, address, etc. The information may be encrypted and/or digitally signed.
- User authentication information, such as an access code, a fingerprint, a retinal scan, etc. The information may be encrypted and/or digitally signed. This can be used to guard against stolen KDs.
    - A use counter for each ticket with a limited number of uses.
-
- An authentication token that contains the Bluetooth address (or a similar, unique network address if another communication technology is used) of the KD, digitally signed by a well known trusted authority. The idea with the token is that such a token is only given to "secure" devices that cannot easily be used to copy tickets with a limited number of uses or to otherwise commit fraudulent acts. The token can be used to certify that the KD behaves in a